

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP04/019221

International filing date: 22 December 2004 (22.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-166706
Filing date: 04 June 2004 (04.06.2004)

Date of receipt at the International Bureau: 24 February 2005 (24.02.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

27.12.2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 4 年 6 月 4 日
Date of Application:

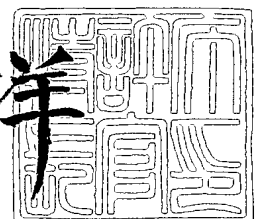
出 願 番 号 特 願 2 0 0 4 - 1 6 6 7 0 6
Application Number:
[ST. 10/C]: [J P 2 0 0 4 - 1 6 6 7 0 6]

出 願 人 三 菱 電 機 株 式 有 限 公 司
Applicant(s):

2 0 0 5 年 2 月 1 4 日

特許庁長官
Commissioner,
Japan Patent Office

小 川 洋



【書類名】 特許願
【整理番号】 551337JP01
【提出日】 平成16年 6月 4日
【あて先】 特許庁長官殿
【国際特許分類】 G01S 5/14
【発明者】
 【住所又は居所】 東京都千代田区丸の内二丁目 2 番 3 号 三菱電機株式会社内
 【氏名】 富樫 昌孝
【特許出願人】
 【識別番号】 000006013
 【氏名又は名称】 三菱電機株式会社
【代理人】
 【識別番号】 100099461
 【弁理士】
 【氏名又は名称】 溝井 章司
【手数料の表示】
 【予納台帳番号】 056177
 【納付金額】 16,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1

【書類名】 特許請求の範囲**【請求項 1】**

情報を処理する情報処理機器と、
情報処理機器の動作環境を証明する電子証明書を発行する証明書発行サーバと、
情報を保管記憶部に保管記憶する情報保管サーバとを備え、
情報処理機器は、証明書発行サーバに対して情報処理機器の動作環境の証明要求を送信し、

証明書発行サーバは、情報処理機器から送信された動作環境の証明要求に基づいて、情報処理機器の動作環境を証明する電子証明書を発行し、

情報処理機器は、証明書発行サーバが発行した電子証明書を受信し、電子証明書と処理情報とに基づく証明書付き情報と、この証明書付き情報を識別する識別情報とを作成して情報保管サーバへ送信し、

情報保管サーバは、情報処理機器から証明書付き情報と識別情報とを受信して保管記憶部に保管するとともに、識別情報を受信して保管記憶部に記憶された証明書付き情報を検索し、検索した証明書付き情報を出力することを特徴とする証明システム。

【請求項 2】

証明書発行サーバは、動作環境として、情報処理機器が動作する時刻を証明することを特徴とする請求項 1 記載の証明システム。

【請求項 3】

証明書発行サーバは、動作環境として、情報処理機器が動作する位置を証明することを特徴とする請求項 1 記載の証明システム。

【請求項 4】

情報処理機器は、現在の時刻を示す時刻情報を取得して、取得した時刻情報を証明書発行サーバに送信し、

証明書発行サーバは、情報処理機器から時刻情報を受信して、その時刻情報が示す時刻にしか得られない一意のデータを時刻情報に付加することにより時刻を証明する電子証明書を発行することを特徴とする請求項 1 記載の証明システム。

【請求項 5】

情報処理機器は、情報処理機器の位置を示す位置情報を取得して、取得した位置情報を証明書発行サーバに送信し、

証明書発行サーバは、情報処理機器から位置情報を受信して、その位置情報が示す位置にいるときにしか得られない一意のデータを位置情報に付加することにより位置を証明する電子証明書を発行することを特徴とする請求項 1 記載の証明システム。

【請求項 6】

証明書発行サーバは、位置情報が示す位置を補正する補正情報を位置情報に付加して電子証明書を発行することを特徴とする請求項 5 記載の証明システム。

【請求項 7】

情報処理機器は、電子証明書と処理情報とをあわせた合成情報を作成し、その合成情報を証明書付き情報として情報保管サーバに送信するとともに、

情報保管サーバは、情報処理機器から合成情報と識別情報とを受信して保管記憶部に保管するとともに、識別情報を含む問い合わせを受信して保管記憶部に記憶された合成情報を検索し、検索した合成情報を出力することを特徴とする請求項 1 記載の証明システム。

【請求項 8】

情報処理機器は、電子証明書と処理情報とをあわせた合成情報を作成し、合成情報のハッシュ値を計算して、そのハッシュ値を証明書付き情報として情報保管サーバに送信するとともに、

情報保管サーバは、情報処理機器からハッシュ値と識別情報とを受信して保管記憶部に記憶するとともに、合成情報を受信してハッシュ値による比較をしてから合成情報を保管記憶部に記憶するとともに、識別情報を含む問い合わせを受信して保管記憶部に記憶された合成情報を検索し、検索した合成情報を出力することを特徴とする請求項 1 記載の証明シス

テム。

【請求項 9】

証明書発行サーバと情報保管サーバとは、同一のサーバであることを特徴とする請求項 1 記載の証明システム。

【請求項 10】

情報処理機器に対して電子証明書を発行する証明書発行サーバにおいて、
情報処理機器の動作環境の証明要求を受信する証明要求受信部と、
証明要求受信部が受信した証明要求に基づいて、情報処理機器の動作環境を証明する電子証明書を発行する証明書発行部と、
証明書発行部が発行した電子証明書を情報処理機器に送信する証明書送信部とを備えたことを特徴とする証明書発行サーバ。

【請求項 11】

証明書発行サーバは、動作環境として、情報処理機器が動作する時刻と位置との少なくともいずれかを証明をすることを特徴とする請求項 10 記載の証明書発行サーバ。

【請求項 12】

情報を処理する情報処理機器において、
情報を処理し処理情報として記憶する情報処理部と、
情報処理部の動作環境を証明する電子証明書を発行する証明書発行サーバに対して情報処理機器の動作環境の証明要求を送信する証明要求部と、
証明要求部が送信した証明要求に対して証明書発行サーバが発行した電子証明書を受信し、電子証明書と処理情報とに基づく証明書付き情報とこの証明書付き情報を識別する識別情報とを作成して出力する情報出力部とを備えたことを特徴とする情報処理機器。

【請求項 13】

上記情報処理機器は、警備保障対象の情報を取得する携帯警備機器であることを特徴とする請求項 12 記載の情報処理機器。

【請求項 14】

情報処理機器から情報処理機器の動作環境が証明された証明書付き情報とこの証明書付き情報を識別する識別情報とを受信する情報受信部と、
情報受信部が受信した証明書付き情報と識別情報とを保管記憶する保管記憶部と、
識別情報を含む問い合わせを受信して保管記憶部に記憶された証明書付き情報を検索し、検索した証明書付き情報を出力することにより情報処理機器の動作環境を証明する証明出力部とを備えたことを特徴とする情報保管サーバ。

【請求項 15】

保管記憶部は、さらに、情報受信部が受信した証明書付き情報と識別情報との受信順番を記憶することを特徴とする請求項 14 記載の情報保管サーバ。

【書類名】明細書

【発明の名称】動作環境を証明する情報処理機器、証明書発行サーバ及び情報保管サーバ並びに証明システム

【技術分野】**【0001】**

本発明は、例えば、警備員が巡回警備を行った地点と時刻とを証明し、また、巡回警備を行った際に映像を撮影した地点と時刻とを証明する情報処理機器、証明書発行サーバ及び情報保管サーバ並びに証明システムに関する。

【背景技術】**【0002】**

従来、施設等の警備は、警備会社の警備員が所定の時刻に所定の地点を巡回して異常の有無を確認することにより行うのが一般的である。その場合、警備の依頼者は、警備員が規定の時刻に規定の地点を巡回したことを確認する必要がある、また、警備会社は規定どおり巡回を行ったことを証明する必要がある。

【0003】

その確認と証明を実現する手段の一つに、予め巡回経路の所定の地点に錠前を設置したボックスを配置しておき、警備員が巡回の過程で、携帯する鍵を用いてボックスの錠前を操作（開錠または施錠の動作）することにより、その地点に来た事実とその時刻を記録に残していく方法がある。

【0004】

しかし、この方法では、巡回経路の追加や変更には、新たなボックスの設置やボックスの移動が必要となることから、容易に対応することができない。また、ボックスの配置されていない経路を巡回する必要が生じたとしても、警備を実施した記録は残らず、後に警備を実施したことを証明することはできない。

【0005】

また、警備員にとっても鍵を常に携帯する必要がある、巡回警備の最中に、本来の警備とは関係のない錠前の操作を行うことの負担が大きい。さらに、錠前の操作に注意が集中する間は、警備が疎かになる可能性もある。

【0006】

前記した錠前に代えて、巡回経路の所定の地点に設置された送信装置から、巡回する警備員が携帯する受信装置に対して送信装置のID情報（位置情報）と時刻情報とを送信し、それにより巡回した事実と巡回した時刻を証明し、それを確認する方法がある。このような方法は、一般的には、タイムスタンプと呼ばれている（特許文献1を参照）。

【0007】

しかし、タイムスタンプでは、位置情報と時刻情報の記録を警備員側の操作により実行することから、タイムスタンプした送信装置のID情報（位置情報）や時刻情報の偽造や改ざんが可能であるという問題がある。

【0008】

この問題と解決するために、警備員側がタイムスタンプを操作するのではなく、警備員が携帯する受信装置が、送信装置から受信した送信装置のID情報（位置情報）と時刻情報とを直ちに第三者が管理するサーバへ送り、サーバが正式なタイムスタンプを実行し保管する方法がある（特許文献2を参照）。

【0009】

しかし、これらタイムスタンプを用いた方法によっても、巡回経路の所定の地点に送信装置を設置しておく必要があることから、前記した巡回経路の追加や変更に対応できないという問題は残る。さらに、後者のタイムスタンプを用いた方法でも、サーバを管理する第三者によるタイムスタンプの偽造や改ざんの問題は発生する可能性がある。

【0010】

巡回警備を行った場合、通常、その状況は記録に残される。しかし、記録は、警備員が注目した対象や特異な状況が、警備員の記憶やメモにもとづいて、文書により報告書とし

て残されることが多い。その結果、記録として残るのは、警備員が注目した部分のみであり、警備員が注目しなかった部分については記録が残らず、後日、必要な情報を得ることが困難な場合があった。また、必要に応じて写真やビデオによる映像の撮影も行われるが、それは正式に地点や時刻を特定し証明できるものではなく、訴訟等においては証拠としての能力がなかった。

【特許文献1】特開昭61-82288号公報

【特許文献2】特開2004-46305号公報

【特許文献3】特開2001-297062号公報

【発明の開示】

【発明が解決しようとする課題】

【0011】

この発明は、例えば、巡回した地点と時刻を証明するための装置を予め設置することなく、また、巡回したことを証明できる地点を事前に定められた地点に限定されることなく、巡回した地点と巡回した時刻を証明する巡回警備の証明システムを提供することを目的とする。また、例えば、証明された地点と時刻の情報が、当事者はもとより第三者によっても偽造や改ざんされないようにすることを目的とする。さらに、例えば、証明された地点と時刻の情報を撮影した映像に付加することにより、映像が撮影された地点と時刻を証明することができるようにすることを目的とする。

【課題を解決するための手段】

【0012】

この発明の証明システムは、情報を処理する情報処理機器と、情報処理機器の動作環境を証明する電子証明書を発行する証明書発行サーバと、情報を保管記憶部の保管記憶する情報保管サーバとを備え、情報処理機器は、証明書発行サーバに対して情報処理機器の動作環境の証明要求を送信し、証明書発行サーバは、情報処理機器から送信された動作環境の証明要求に基づいて、情報処理機器の動作環境を証明する電子証明書を発行し、情報処理機器は、証明書発行サーバが発行した電子証明書を受信し、電子証明書と処理情報とに基づく証明書付き情報とこの証明書付き情報を識別する識別情報とを作成して情報保管サーバへ送信し、情報保管サーバは、情報処理機器から証明書付き情報と識別情報とを受信して保管記憶部に保管するとともに、識別情報を受信して保管記憶部に記憶された証明書付き情報を検索し検索した証明書付き情報を出力することとした。

【発明の効果】

【0013】

本発明によれば、情報処理機器と、証明書発行サーバと、情報保管サーバとから証明システムを構成することができる。また、証明システムの情報処理機器からの証明要求にもとづいて証明書発行サーバは、情報処理機器の動作環境を証明する電子証明書を発行することができ、情報処理機器は処理情報と電子証明書とを証明付き情報とした上で、それを識別する識別情報と共に情報保管サーバへ送り、情報保管サーバは証明付き情報を識別情報ごとに保管することができる。後日、情報保管サーバから識別情報にもとづいて証明付き情報を検索して得ることができる。その結果、証明システムは、情報処理装置が処理情報を処理した際の動作環境を証明することが可能となる。

【発明を実施するための最良の形態】

【0014】

実施の形態1.

実施の形態1では、警備員が巡回警備を行った際に映像を撮影した地点（位置とも表現している）と時刻（本実施の形態では日付を含むものとする）の証明を行い、後に映像を撮影した地点と時刻が本当であるか否かを確認することができる実施の形態について説明する。

【0015】

図1は、実施の形態1における巡回警備を行った際に映像を撮影した地点と時刻を証明するために必要となる構成を示す図である。

巡回警備を行った地点と時刻を証明するためには、地球上の任意の地点の位置情報を提供する全地球測位システム（GPS：Global Positioning System）衛星10と、地球上の気象（具体的には雲の状況）を撮影し、その映像を提供する気象衛星20と、巡回警備を行う警備員が巡回時に携帯する情報処理機器30（ここではビデオカメラが情報処理機器の機能を兼ね備えるものとする）と、証明書発行センタに備えられており、時刻情報と位置情報との証明を行う証明書発行サーバ40と、情報保管センタに備えられており、証明された位置情報と時刻情報とそれらを添付した処理情報である映像を保管する情報保管サーバ50と、映像を撮影した地点と時刻が本当であるか否かを検証する検証装置60と、情報処理機器30と証明書発行サーバ40と情報保管サーバ50と検証装置60とを相互に接続するネットワーク70とが存在する。

【0016】

このうち、本実施の形態に係る巡回警備の証明システムの構成を図2に示す。

巡回警備の証明システムは、情報を処理する情報処理機器30と、情報処理機器の動作環境を証明する電子証明書を発行する証明書発行サーバ40と、情報を保管記憶部（後述する）に保管記憶する情報保管サーバ50とを備える。

【0017】

情報処理機器30は、ビデオカメラの機能を兼ね備えており、巡回警備の際に異常の有無等の状況を撮影すると共に、撮影した地点の位置情報と時刻情報をGPS衛星10から取得する。

【0018】

なお、本実施の形態でいう「動作環境」とは、警備員がビデオカメラの機能を兼ね備える情報処理機器30を用いて映像を撮影した地点と時刻とを意味している。また、本実施の形態でいう「処理情報」とは、情報処理機器30が処理する情報、つまり情報処理機器30がビデオカメラの機能を兼ね備えていることから、撮影した映像が処理情報に相当する。

【0019】

証明書発行サーバ40は、動作環境として、情報処理機器30が動作する時刻と位置とを証明する。または、証明書発行サーバ40は、動作環境として、情報処理機器30が動作する時刻と位置との少なくともいずれかを証明をする。

【0020】

そのために証明書発行サーバ40は、情報処理機器30から位置情報と時刻情報を受信し、それらを「位置情報がその地点で得られたことを証明する方法」（後述する）と後述する「時刻情報がその時刻に得られたことを証明する方法」（後述する）を用いてそれぞれ証明し、証明された位置情報と時刻情報を電子証明書として情報処理機器30へ送信する。

【0021】

情報保管サーバ50は、情報処理機器30から処理情報、つまり巡回時に撮影した映像と共に証明された位置情報と時刻情報の電子証明書を受信して保管する。また、情報保管サーバ50は、証明書発行サーバ40に対して、証明された位置情報と時刻情報の電子証明書が、証明書発行サーバ40が発行した正当な証明書であるか否に関する問い合わせを行う。

【0022】

情報処理機器30は、証明書発行サーバ40に対して情報処理機器30の動作環境の証明要求を送信する。証明書発行サーバ40は、情報処理機器30から送信された動作環境の証明要求に基づいて、情報処理機器30の動作環境を証明する電子証明書を発行する。情報処理機器30は、証明書発行サーバ40が発行した電子証明書を受信し、電子証明書と処理情報とに基づく証明書付き情報とこの証明書付き情報を識別する識別情報とを作成して情報保管サーバ50へ送信する。情報保管サーバ50は、情報処理機器30から証明書付き情報と識別情報とを受信して保管記憶部に保管するとともに、検証要求の問い合わせ時、識別情報を受信して保管記憶部に記憶された証明書付き情報を検索して証明書付き

情報を出力する。

【0023】

このため情報処理機器30は、警備保障対象の情報を取得する携帯警備機器であってもよく、例えば、カメラ、ビデオカメラ、録音機などを利用することができる。

【0024】

識別情報は、個々の証明書付き情報がどの情報処理装置から、いつ送られたかをそれぞれ識別するための情報である。情報保管サーバ50は、複数の情報処理装置から送られた多数の証明書付き情報を記憶することがあることから、それぞれの証明書付き情報を識別するために付与される。

【0025】

図3は情報処理機器30の構成を示す図である。

情報を処理する情報処理機器30において、情報を処理し処理情報として記憶する情報処理部31と、情報処理部31の動作環境を証明する電子証明書を発行する証明書発行サーバ40に対して情報処理機器30の動作環境の証明要求を送信する証明要求部32と、証明要求部32が送信した証明要求に対して証明書発行サーバ40が発行した電子証明書を受信し、電子証明書と処理情報とに基づく証明書付き情報とこの証明書付き情報を識別する識別情報とを作成して出力する情報出力部33とを備える。さらに、情報処理機器30は、GPS衛星10から動作環境を規定する位置情報と時刻情報を受信する位置時刻情報受信部34を備える。

【0026】

図4は証明書発行サーバ40の構成を示す図である。

情報処理機器30に対して電子証明書を発行する証明書発行サーバ40において、情報処理機器30の動作環境の証明要求を受信する証明要求受信部41と、証明要求受信部41が受信した証明要求に基づいて、情報処理機器30の動作環境を証明する電子証明書を発行する証明書発行部42と、証明書発行部42が発行した電子証明書を情報処理機器30に送信する証明書送信部43とを備える。さらに、証明書発行サーバ40は、気象衛星2から気象情報を受信する気象情報受信部44と、証明要求受信部41が受信した証明要求に含まれる位置情報を正確な位置情報に補正する位置情報補正部45とを備える。

【0027】

図5は情報保管サーバ50の構成を示す図である。

情報保管サーバ50は、情報処理機器30から情報処理機器30の動作環境が証明された証明書付き情報とこの証明書付き情報を識別する識別情報とを受信する情報受信部51と、情報受信部51が受信した証明書付き情報と識別情報とを保管記憶する保管記憶部53と、識別情報を含む問い合わせを受信して保管記憶部53に記憶された証明書付き情報を検索し検索した証明書付き情報を出力することにより情報処理機器30の動作環境を証明する証明出力部52とを備える。

【0028】

保管記憶部53は、さらに、情報受信部が受信した証明書付き情報と識別情報との受信順番を記憶する。

【0029】

次に、巡回警備の証明システムを用いて巡回警備した地点と時刻を証明する処理を説明する。以下では、巡回警備を行った地点と時刻の両方を証明する場合について説明しているが、時刻だけを証明する場合、または、地点だけを証明する場合であってもよい。

【0030】

情報処理機器30は、現在の時刻を示す時刻情報と情報処理機器30の位置を示す位置情報とを位置時刻情報受信部34により取得して、取得した時刻情報と位置情報とを証明要求部32により証明書発行サーバ40に送信する。

【0031】

また、証明書発行サーバ40は、証明要求受信部41により情報処理機器30から時刻情報と位置情報を受信し、証明書発行部42は、その時刻情報が示す時刻にしか得られな

い一意のデータを時刻情報に付加し、その位置情報が示す位置にいるときにしか得られない一意のデータを位置情報に付加することにより時刻と位置を証明する電子証明書を発行する。

【0032】

その際、証明書発行サーバ40の位置情報補正部45は、位置情報が示す位置を補正する補正情報を位置情報に付加して電子証明書を発行する。

【0033】

情報処理機器30の情報出力部33は、証明書発行サーバ40の証明書送信部43から受信した電子証明書と、情報処理部31が得た処理情報とを合わせた合成情報を作成し、その合成情報を証明書付き情報として情報保管サーバ50に送信する。

【0034】

情報保管サーバ50の情報受信部51は、情報処理機器30から証明書付き情報とその証明書付き情報の識別情報とを受信して保管記憶部53に保管するとともに、検証要求の問い合わせ時、識別情報を含む問い合わせを受信して保管記憶部53に記憶された証明書付き情報を検索し、検索した証明書付き情報を出力する。

【0035】

あるいは、情報処理機器30の情報出力部33は、電子証明書と処理情報とをあわせた合成情報を作成し、合成情報のハッシュ値を計算して、そのハッシュ値を証明書付き情報として情報保管サーバ50に送信してもよい。

【0036】

情報保管サーバ50の情報受信部51は、情報処理機器30から合成情報のハッシュ値である証明書付き情報とその証明書付き情報の識別情報とを受信して保管記憶部に記憶するとともに、後日、合成情報を受信して、そのハッシュ値を計算し、先に受信していた証明書付き情報と比較をして、一致した場合、合成情報を識別情報に対応させて保管記憶部53に記憶する。検証時には、識別情報を含む問合せを受信し、保管記憶部53に記憶された合成情報を検索して、検索した合成情報を出力する。この場合には、図5に示す「検索した証明書付き情報」は、「検索した合成情報」となる。

【0037】

なお、証明書発行サーバ40と情報保管サーバ50とは、同一のサーバであってもよい。

【0038】

警備員が巡回警備を行った際に映像を撮影した地点と時刻を証明するための処理をさらに具体的に説明する。図6は、警備員が巡回警備を行った際に撮影した映像の撮影した地点と時刻を証明する処理を示す図である。

【0039】

警備員は、各地点の巡回警備を行いながらビデオカメラの機能を兼ね備える情報処理機器30を用いて各地点の警備状況を撮影する。その間、情報処理機器30は、GPS衛星10から、その地点での位置情報と時刻情報を受信し、改ざんや漏洩を防止するためにそれらを暗号化した上で、図示しない無線LANや携帯電話等の無線回線とネットワーク70を経由して、証明書発行サーバ40へ送信する（ステップS101）。

【0040】

この処理は、警備員による操作により実行を開始してもよいし、情報処理機器30が一定の時間間隔で自動的に開始してもよい。また、GPS衛星10からの位置情報と時刻情報の受信は常時実行しており、受信した位置情報と時刻情報の証明書発行サーバ40へ送信のみを警備員の操作や一定の時間間隔などで実行してもよい。

【0041】

証明書発行サーバ40は、情報処理機器30から受信した暗号化した位置情報と時刻情報を復号した上で（ステップS102）、位置情報に含まれる位置をより正確にするための補正処理を行う（ステップS103）。その後、証明書発行サーバ40は、「位置情報がその地点において得られたことを証明する方法」（後述する）と、「時刻情報がその時

刻に得られたことを証明する方法」(後述する)を行う。

【0042】

ここで、「位置情報がその地点において得られたことを証明する方法」について説明する。情報処理機器30の位置時刻情報受信部34は、電波を受信可能な複数のGPS衛星10から測位コードと搬送波との組を受信する。情報処理機器30の証明要求部32は、受信した測位コードと搬送波との組を、受信した測位衛星の識別記号と共に、自身のIDを暗号鍵にして暗号化した上で、位置情報として証明書発行サーバ40に送信する。

【0043】

その際、位置情報の正確性を付加するために、GPS衛星10から得た位置情報の他に、気温、湿度等、その地点で得られる自然現象情報、通信手段によって得られる基地局情報等の環境情報を取得し、証明書発行サーバ40に送付することで、その地点であることが強化される。また、証明書発行サーバ40との暗号手段を用いたやりとりにより、常に取得した全データを送付するだけでなく、暗号手段的に選択されたデータだけを送付する方式によりなりすましの防止を強化する。

【0044】

証明書発行サーバ40の証明要求受信部41は、情報処理機器30から位置情報を受信し、復号した後、証明書発行部42へ送る。証明書発行部42は、復号された測位コードと搬送波と測位衛星の識別番号とに基づいて、位置情報の証明を要求した情報処理機器30の位置を算出し、証明書発行サーバ40が備えるデータベースに保管する(ステップS104)。この位置の算出には、一般に知られている方式を利用することができる。次に、証明書発行部42は、算出した情報処理機器30の位置を証明する証明書を作成し、改ざん防止のためのコピーガードを施した上で、情報処理機器30へ送信する。その際、証明書は端末に固有のIDに対する証明書として作成される。また、コピーガードの方式には、一般に知られている方式を利用することができる。

【0045】

このようにその時刻にその地点でしか得ることができないGPS衛星10の識別番号と測位コードと搬送波とから位置を算出することにより、その時刻にそこに存在したことを証明している。

【0046】

ここで、「時刻情報がその地点において得られたことを証明する方法」について説明する。時刻情報がその時刻に得られたことの証明には、例えば、特許文献3に記載された時刻を証明する発明を利用する。その発明は、証明したい時刻と同時刻に発生した自然現象(ここでは気象情報)を証明したい時刻情報に付帯させることにより、時刻が本当であることを証明する。

【0047】

証明書発行サーバ40は、復号した時刻情報と同じ時刻に気象衛星が撮影した気象情報(具体的には雲の状況)を受信して(ステップS105)、時刻情報に付帯して証明された時刻情報として備えるデータベースに保管する(ステップS106)。

【0048】

証明書発行サーバ40は、ハッシュ関数を用いて、証明された時刻情報と証明された位置情報のハッシュ値を生成する。このハッシュ値は、自然現象の情報と時刻情報と位置情報とから一意に決定される値であり、ハッシュ関数が一方向性関数であることから、元の値に戻すことはできない。ハッシュ値は、証明書発行サーバ40により位置情報と時刻情報の電子証明書として情報処理機器30へ送信される(ステップS107)。

【0049】

情報処理機器30は、撮影した映像のハッシュ値を生成し(ステップS108)、証明書発行サーバ40から受信した位置情報と時刻情報の電子証明書を撮影した映像のハッシュ値に付加して証明書付き情報を生成し、識別情報と共に情報保管サーバ50へ送信する(ステップS109)。

【0050】

情報処理機器 30 から証明書付き情報を受信した情報保管サーバ 50 は、受信した順番などの固有の番号をそれに付与した後、情報処理機器 30 が備えるデータベースに記憶して保管する（ステップ S110）。その後、情報保管サーバ 50 は、証明書発行サーバ 40 に対して、受信した証明書付き情報に含まれる証明された位置情報と時刻情報とが、証明書発行サーバ 40 により作成されたものであるか否かの確認を要求する（ステップ S111）。

【0051】

情報保管サーバ 50 から確認を要求された証明書発行サーバ 40 は、受信した証明された位置情報と時刻情報が、自分自身が作成した証明された位置情報と時刻情報であるか否かを確認し（ステップ S112）、その結果を情報保管サーバ 50 に送信する（ステップ S113）。

【0052】

その後、警備員が巡回警備を行った際に撮影した映像の撮影した地点と時刻を検証する必要がある場合、検証者は検証装置 60 を用いて情報保管サーバ 50 に対してその問い合わせを行い（ステップ S114）、情報保管サーバ 50 の検証を行ってその結果を検証装置 60 へ送信する（ステップ S115）。検証装置 60 は、検証結果を受信し、検証者はその内容を確認する（ステップ S116）。

【0053】

本実施の形態によれば、情報処理機器は、証明書発行サーバが発行した情報処理機器の動作環境を証明する電子証明書を用いることによって、処理情報を処理した動作環境を証明することができる。また、処理情報とそれを処理する情報処理機器の動作環境を情報保管サーバに保管することにより、情報処理機器が処理情報を処理した動作環境を検証することができる。

【0054】

本実施の形態によれば、巡回警備の際に映像を撮影した地点と時刻とが真実であることを証明することが可能となる。その結果、撮影した映像に証拠としての能力を持たせることができ、裁判等で利用することが可能となる。

【0055】

本実施の形態によれば、情報処理機器は、証明書発行サーバが発行した情報処理機器が動作する時刻を証明する電子証明書を用いることによって、処理情報を処理した時刻を証明することができる。

【0056】

本実施の形態によれば、情報処理機器は、証明書発行サーバが発行した情報処理機器が動作する位置を証明する電子証明書を用いることによって、処理情報を処理した位置を証明することができる。

【0057】

本実施の形態によれば、情報処理機器は、証明書発行サーバが、その時刻でしか得られない一意のデータを時刻情報に付加した証明書を用いることによって、処理情報を処理した時刻を証明することができる。

【0058】

本実施の形態によれば、情報処理機器は、証明書発行サーバが、情報処理機器の存在する位置でしか得られない一意のデータを位置情報に付加した証明書を用いることによって、処理情報を処理した位置を証明することができる。

【0059】

本実施の形態によれば、情報処理機器は、位置情報が示す位置を補正する補正情報を用いることによって、処理情報を処理した位置をより正確な位置で証明することができる。

【0060】

本実施の形態によれば、情報処理機器が、処理情報とそれを処理した時刻と位置とを証明する電子証明書を情報保管サーバに送信して保管しておくことにより、後日、検証者は、処理情報を処理した時刻と位置の真偽を検証することができる。

【0061】

本実施の形態によれば、情報処理機器は、情報保管サーバに送信して保管するデータを、処理情報とそれを処理した時刻と位置とを証明する電子証明書とのハッシュ値とすることにより、送信し保管するデータの量を減少させることができる。また、送信中のデータの漏洩と改ざんを防止することができる。

【0062】

本実施の形態によれば、証明システムの構成を簡単化することができ、また、システムの構築や運用に必要な費用を低減することができる。

【0063】

本実施の形態によれば、証明システムの証明書発行サーバを、証明要求受信部と、証明書発行部と、証明書送信部とから構成することができる。

【0064】

本実施の形態によれば、証明書発行サーバは、情報処理機器が動作する時刻と位置を証明することができる。

【0065】

本実施の形態によれば、証明システムの情報処理機器を、情報処理部と、証明要求部と、情報出力部とから構成することができる。

【0066】

本実施の形態によれば、情報処理機器として、巡回警備の際に警備対象の情報を取得する携帯警備機器を用いることができる。

【0067】

本実施の形態によれば、証明システムの情報保管サーバを、情報受信部と、保管記憶部と、証明出力部とから構成することができる。

【0068】

本実施の形態によれば、情報保管サーバにおいて、証明書付き情報と識別情報とを受信した順番で管理することができ、また検索することが可能となる。

【0069】

本実施の形態によれば、情報処理機器から送信される位置情報と時刻情報を用いることにより、リアルタイムで巡回警備を行っている警備員の巡回位置や巡回軌跡、警備の進行状況を知ることができる。

【0070】

本実施の形態によれば、映像が証明された位置情報と時間情報を付帯することにより証拠としての能力を備えれば、事件、事故の早期解決や裁判の早期終了が期待できる。

【0071】

従来の映像は、物理的なフィルムに物理的な記録により撮影され、それが証拠としての価値を生み出していた。しかし、デジタルデータでは、物理的な証明が少なく、証拠能力が低下していた。そこに自然現象が生み出すデータを付加することで物理的な連携をとり、その証明データを受取り対タンパ性を持つ端末により暗号化、署名されたデータは証明力が向上し、証拠としての証明力を確保することが可能な保管方式を構築できる。

【0072】

なお、本実施形態は、巡回監視における巡回警備手段の一方式であって、巡回した位置の特定と、特定した位置を証明するための情報を取得する機器を携帯し、その機器により収集した情報により巡回位置とその時刻の証明し、さらに、その地点の映像を静止画、動画で撮影することにより、巡回地点の警備を実施したことを証明し、さらに静止画、映像を撮影した情報、録音した音声に改ざん防止の手段を加えることにより、巡回位置、時刻での状況報告を実施した静止画、動画を報告、証拠として取り扱うことを可能とする巡回手段である。

【0073】

また、巡回警備に携帯する端末は、映像、画像の撮影手段と、音声の録音手段と、衛星から発信される、その時刻にその位置だけでしか入手できない情報とを取得し、その位置

を証明するために衛星の位置情報を入手する衛星情報の入手手段と、その情報を情報保管サーバに送信する機能と、証明書発行サーバから送信される時刻の証明情報を入手する通信手段と、入手した情報を保管する手段と、入手した情報を撮影した画像データに埋めこむ手段と、その端末が他の端末と認識できる機能を有する。

【0074】

巡回警備における報告を、巡回者の巡回した位置で、映像を撮影した位置と時間を証明することにより、映像、静止画、音声を状況証拠として報告することを可能とする。

【0075】

巡回警備における巡回者の位置を通信によりセンタに逐一報告することで、巡回者の巡回軌跡を証明し、センタ側で巡回者の位置を把握する。

【0076】

映像を撮影する機器は、証明書発行サーバより送付された時刻と位置を証明する電子証明書を保持し、その電子証明書と撮影したデータを組合せ、電子署名を加えることで改ざんの防止をする。そのデータを情報保管サーバに送信する。情報保管サーバは受信した順に番号をつけ保管することにより、受信した画像がその日時に以前に撮影されたことを証明する。

さらに、情報保管サーバから証明書発行サーバに、登録機器へ時刻と位置を証明する電子証明書を送付したかを確認する。さらに、このときに順次番号を証明書発行サーバに送信するか、または、番号を外部へ公開することでより証明力を高めることができる。

【0077】

証明書発行サーバと情報保管サーバを分離することにより、デジタルデータ運営を独立した管理のもとに実行可能となり、外部への秘匿性を保った運営管理が可能となる。

【0078】

巡回警備における報告は、視覚情報を口頭や文字に置き換えて報告していたが、時刻と位置および改ざんされないことを保証した映像情報と音声情報による報告が可能となり、リアルタイムに保証された情報の提供が可能となる。

【0079】

巡回警備を管理する集中指令センタや顧客に対し、リアルタイムに位置、時間を保証した映像、音声を送付するだけで位置情報、時間情報を同時に送付する必要がなくなくなり、緊急な状態でも防災、防犯、事故の専門家の指示を適切な情報で仰ぐことにより、事故、災害に対する指示を受けながら作業が可能となる。

【0080】

この方式をロボットにそのまま活用し、位置情報、時間情報を証明した映像、音声を録画、送信する機能を持たせることで、人間が不可能な警備、防災対策に対応が可能となる。

【0081】

警備車両の位置と時刻の証明による管理、警備員の位置と時刻の証明によるセンタでの集中管理を行うことで全車両、全警備員の位置情報を管理し、緊急時の応援に活用する。

【0082】

映像を撮影する機器に自動的に情報発信する機能を設けることで、警備員の安全確認、活動状況を把握する。

【0083】

機器を自動更新する際に、暗号情報を変更することで撮影機器のなりすましを防ぎ、電子データ撮影の安全性を確保する。

【0084】

機器に対タンパ性を持たせ、分解、改造のために部品の取り外し等を行った場合に全ての機能を失う構造として利用することで、安全な利用を確保する。

【0085】

実施の形態 2.

実施の形態 2 では、警備員が巡回警備を規定どおり行った事実を証明するために、巡回

警備を行った地点と時刻を証明する実施の形態について説明する。本実施形態では、警備員が、その時刻にその地点にいたことが証明できればよいのであるから、その時刻にその地点でしか得ることができない位置情報と時刻情報を、情報処理機器により取得して保持していることを示せばよい。

【0086】

警備員が巡回警備を行った地点と時刻を証明するのに必要な構成は、実施の形態1において図1に示す構成と同じである。また、利用する証明システムも実施の形態1において図1に示す構成と同じである。さらに、利用する各機器の機能と構成も同じである。

【0087】

以下、警備員が巡回警備を行った地点と時刻を証明するための処理について説明する。図7は、警備員が巡回警備を行った地点と時刻を証明する処理を示す図である。

【0088】

警備員は、事前準備として情報処理機器30に、自信の識別情報(ID情報)を設定しておく。また、情報処理機器自体も識別情報(ID情報)を記憶しているものとする。

【0089】

警備員は、情報処理機器30を携帯して各地点の巡回警備を行う。その間、情報処理機器30は、GPS衛星10から、その地点での位置情報と時刻情報を受信し、改ざんや漏洩を防止するためにそれらを暗号化した上で、図示しない無線LANや携帯電話等の無線回線とネットワーク70を経由して、証明書発行サーバ40へ送信する(ステップS201)。

【0090】

この処理は、警備員による操作により実行を開始してもよいし、情報処理機器30が一定の時間間隔で自動的に開始してもよい。また、GPS衛星10からの位置情報と時刻情報の受信は常時実行しており、受信した位置情報と時刻情報の証明書発行サーバ40へ送信のみを警備員の操作や一定の時間間隔などで実行してもよい。

【0091】

証明書発行サーバ40は、情報処理機器30から受信した暗号化した位置情報と時刻情報を復号した上で(ステップS202)、位置情報に含まれる位置をより正確にするための補正処理を行う(ステップS203)。その後、証明書発行サーバ40は、位置情報がその位置において得られたことを証明する方法と、時刻情報がその時刻に得られたことを証明する方法を実行する。

【0092】

位置情報がその地点で得られたことを証明する方法は、実施の形態1と同様である(ステップS204は実施の形態1のステップS104と同じである)。また、時刻情報がその時刻に得られてことを証明する方法は、実施の形態1と同様である(ステップS205は実施の形態1のステップS105と同じであり、ステップS206は同ステップS106と同じである)。

【0093】

証明書発行サーバ40は、ハッシュ関数を用いて、自然現象の情報を含む証明された位置情報と証明された時刻情報のハッシュ値を生成する。生成したハッシュ値は、証明書発行サーバ40により位置情報と時刻情報の電子証明書として情報処理機器30へ送信される(ステップS207)。

【0094】

証明書発行サーバ40から位置情報と時刻情報の電子証明書を受信した情報処理機器30は、警備員の識別情報と情報処理機器30の識別情報とにそれを付加した証明付き情報を生成し、証明書付き情報を識別するための識別情報と共に、情報保管サーバ50へ送信する(ステップS208)。

【0095】

情報処理機器30から証明付き情報またはそのハッシュ値を受信した情報保管サーバ50は、受信した順番などの固有の番号をそれに付与した後、情報処理機器30が備えるデ

ータベースに記憶して保管する（ステップS209）。その後、情報保管サーバ50は、証明書発行サーバ40に対して、受信した位置情報と時刻情報が証明書発行サーバ40により作成されたものであるか否かの確認を要求する（ステップS210）。

【0096】

情報保管サーバ50から確認を要求された証明書発行サーバ40は、証明された位置情報と時刻情報の正当性を確認し（ステップS211）、その結果を情報保管サーバ50に送信する（ステップS212）。

【0097】

その後、警備員が巡回警備を行った地点と時刻を検証する必要がある場合、検証者は検証装置60を用いて情報保管サーバ50に対してその問い合わせを行い（ステップS213）、情報保管サーバ50の検証を行ってその結果を検証装置60へ送信する（ステップS214）。検証装置60は、検証結果を受信し、検証者はその内容を確認する（ステップS215）。

【0098】

本実施の形態によれば、巡回した地点と時刻を証明するための装置を予め設置することなく、また、巡回したことを証明できる地点を、事前に定められた地点に限定されることなく、巡回した地点と巡回した時刻を証明することができる。また、証明された地点と時刻の情報は、当事者はもとより第三者によっても偽造や改ざんされない。

【0099】

以上、本発明を適用した実施の形態について説明したが、本発明は前記した実施の形態に限定されるものではない。

【0100】

前記した各実施形態において、情報処理機器30と、証明書発行サーバ40と、情報保管サーバとは、コンピュータによって実現できるものである。

【0101】

図示していないが、情報処理機器30と、証明書発行サーバ40と、情報保管サーバとは、プログラムを実行するCPU（Central Processing Unit）を備えている。CPUは、例えば、バスを介して、ROM（Read Only Memory）、RAM（Random Access Memory）、通信ボード、表示装置、キーボード、マウス、FDD（Flexible Disc Drive）、CDD（Compact Disc Drive）、磁気ディスク装置、光ディスク装置、プリンタ装置、スキャナ装置等と接続されている。

【0102】

RAMは、揮発性メモリの一例である。ROM、FDD、CDD、磁気ディスク装置、光ディスク装置は、不揮発性メモリの一例である。これらは、記憶装置あるいは記憶部の一例である。

【0103】

前記した各実施形態の情報処理機器30と、証明書発行サーバ40と、情報保管サーバとが扱う情報は、記憶装置あるいは記憶部により記録され、読み出されるものである。

【0104】

通信ボードは、例えば、LAN、インターネット、あるいはISDN（Integrated Services Digital Network）等に接続されている。

【0105】

磁気ディスク装置には、オペレーティングシステム（OS）、ウィンドウシステム、プログラム群、ファイル群が記憶されている。プログラム群は、CPU、OS、ウィンドウシステムにより実行される。

【0106】

情報管理装置2、情報アクセス装置3は、一部あるいはすべてをコンピュータで動作可能なプログラムにより構成しても構わない。あるいは、ROMに記憶されたファームウェアで実現されていても構わない。あるいは、ソフトウェアとハードウェア、あるいは、ソ

フトウェアとハードウェアとファームウェアとの組み合わせで実施されても構わない。

【0107】

プログラム群には、実施形態の説明において「～部」として説明した処理をCPUに実行させるプログラムが含まれる。これらのプログラムは、例えば、C言語やHTMLやSGMLやXMLなどのコンピュータ言語により作成される。

【0108】

前記したプログラムは、磁気ディスク装置、FD (Flexible Disc)、光ディスク、CD (Compact Disc)、MD (Mini Disc)、DVD (Digital Versatile Disc) 等のその他の記録媒体に記憶され、CPUにより読み出され実行される。

【図面の簡単な説明】

【0109】

【図1】実施の形態1における巡回警備を行った際に映像を撮影した地点と時刻を証明するために必要となる構成を示す図である。

【図2】実施の形態1における巡回警備の証明システムの構成を示す図である。

【図3】実施の形態1における情報処理機器の構成を示す図である。

【図4】実施の形態1における証明書発行サーバの構成を示す図である。

【図5】実施の形態1における情報保管サーバの構成を示す図である。

【図6】実施の形態1における巡回警備の証明システムでの巡回警備を行った際に映像を撮影した地点と時刻とを証明する処理を示す図である。

【図7】実施の形態2における巡回警備の証明システムでの巡回警備を行った地点と時刻を証明する処理を示す図である。

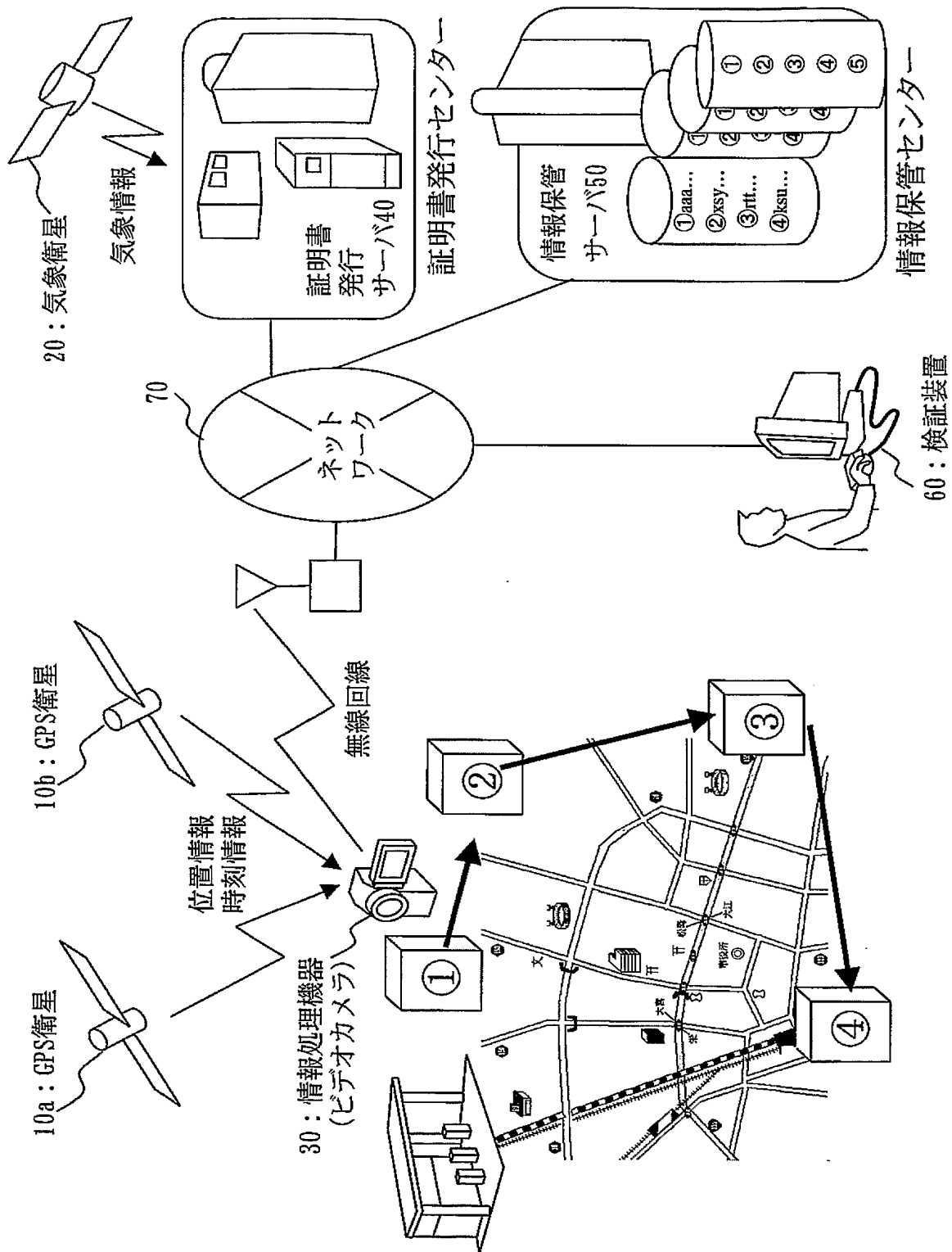
【符号の説明】

【0110】

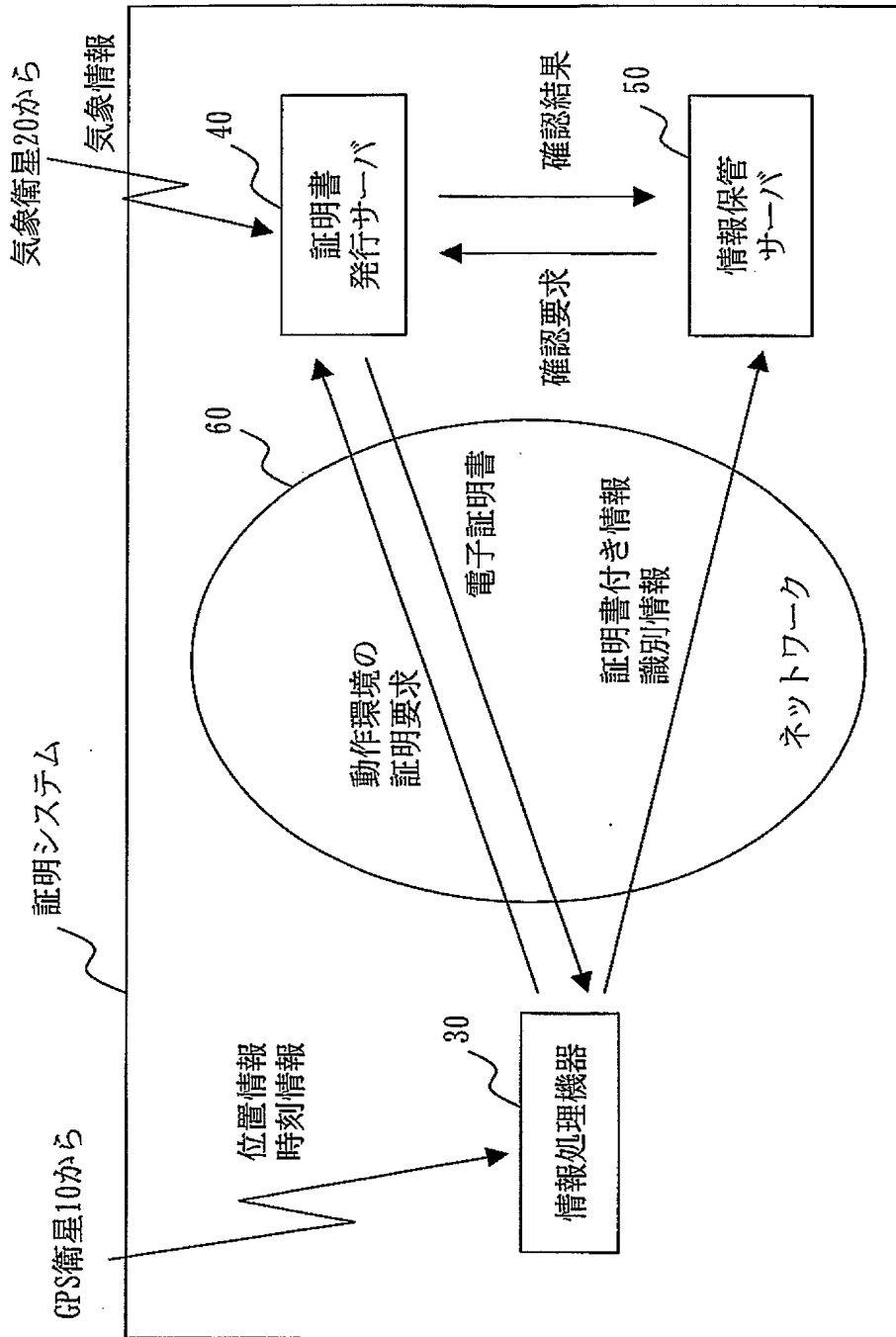
10 GPS衛星、20 気象衛星、30 情報処理機器、31 情報処理部、32 証明要求部、33 情報出力部、34 位置時刻情報受信部、40 証明書発行サーバ、41 証明要求受信部、42 証明書発行部、43 証明書送信部、44 気象情報受信部、45 位置情報補正部、50 情報保管サーバ、51 情報受信部、52 証明出力部、53 保管記憶部、60 検証装置、70 ネットワーク。

【書類名】 図面

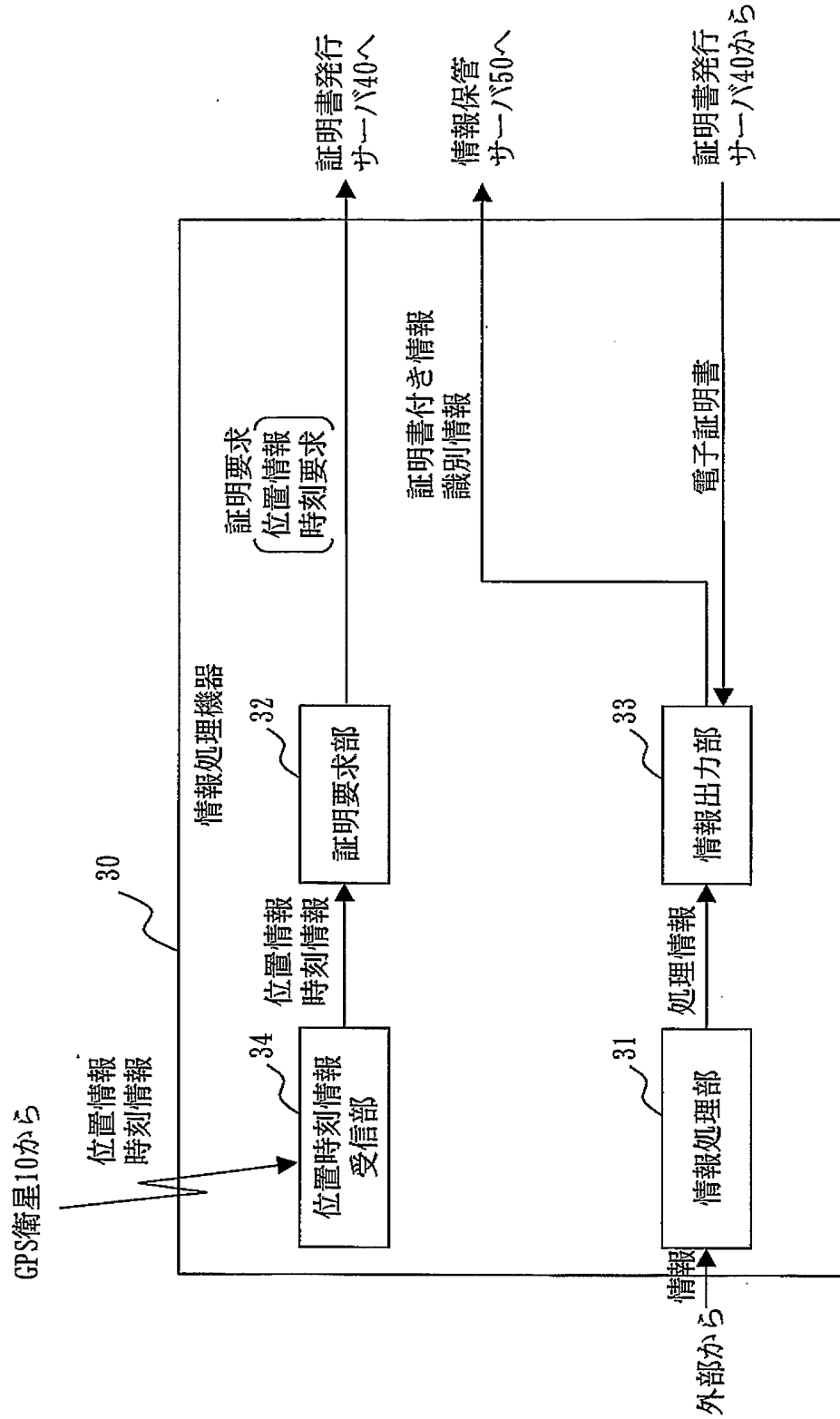
【図 1】



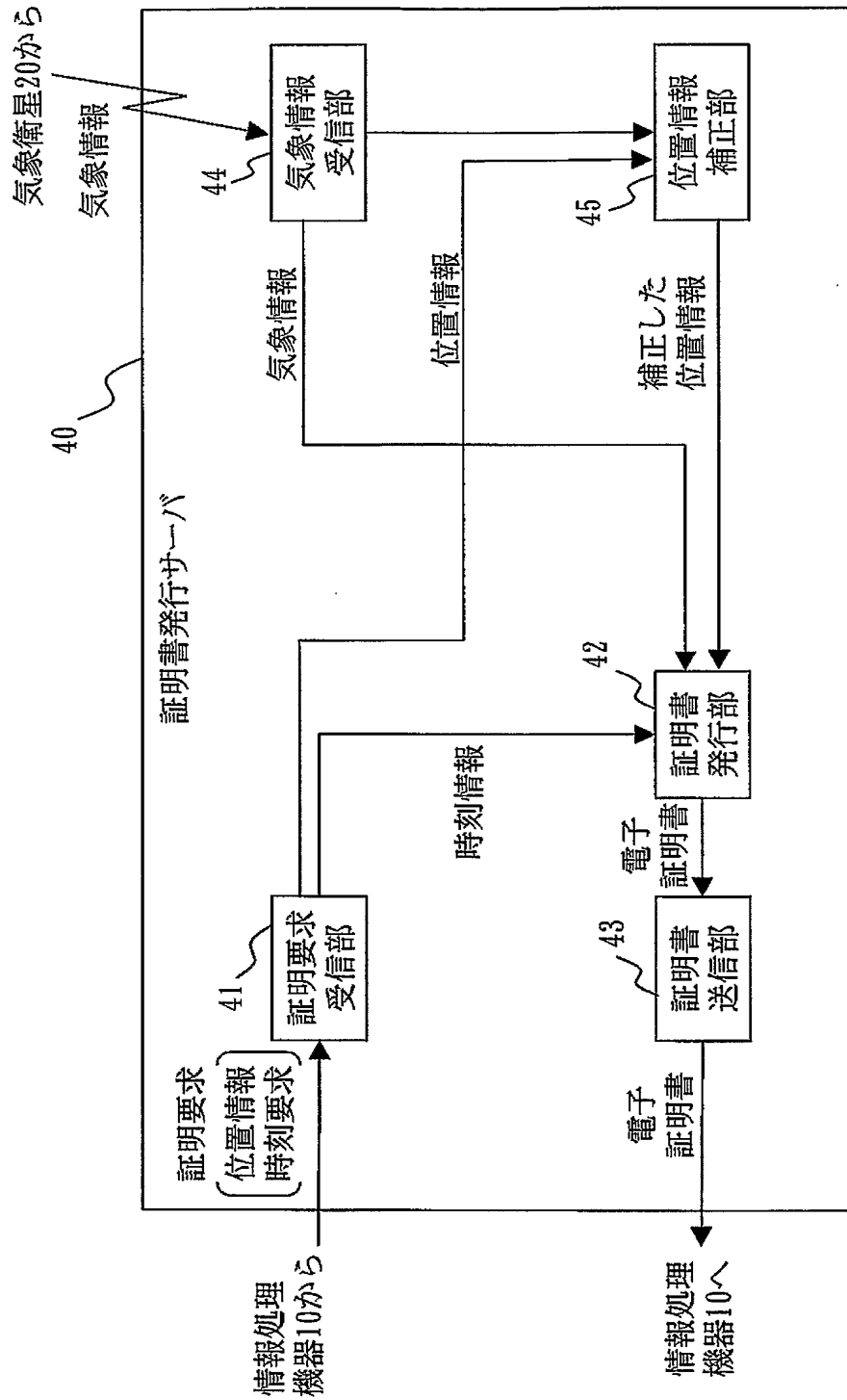
【図 2】



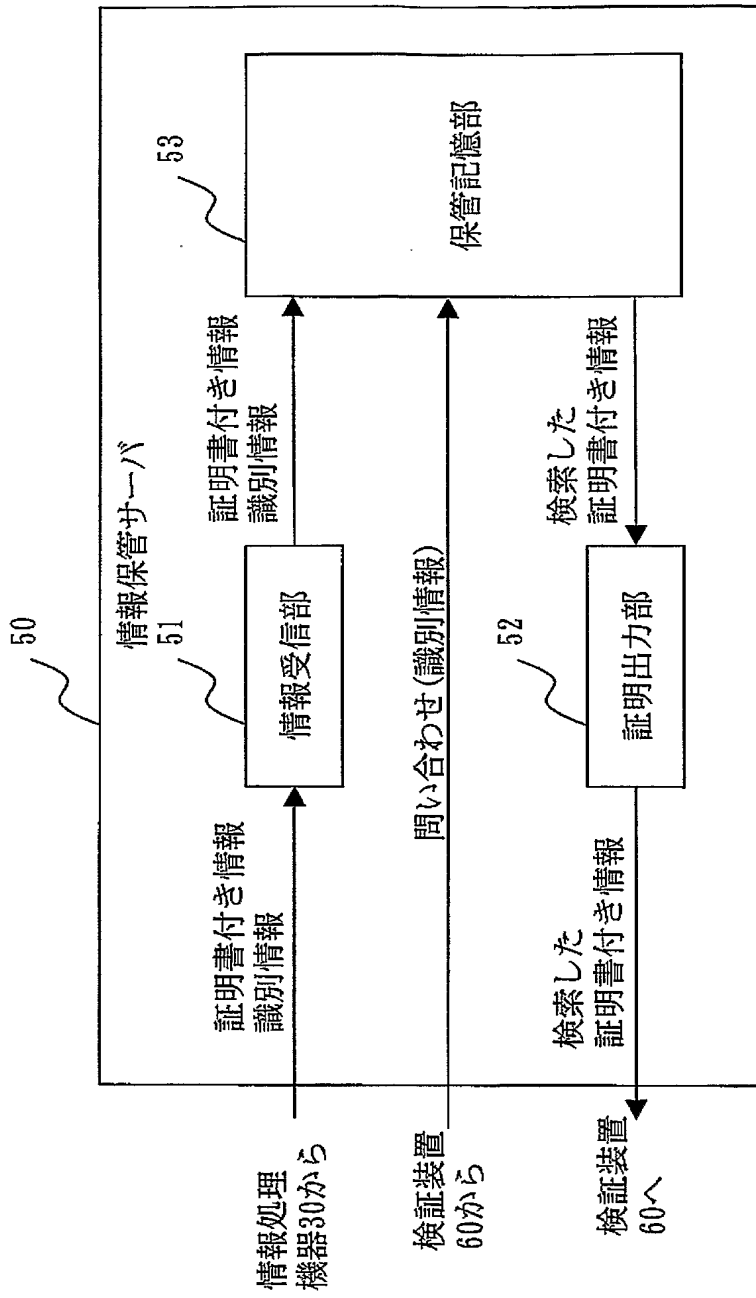
【図 3】



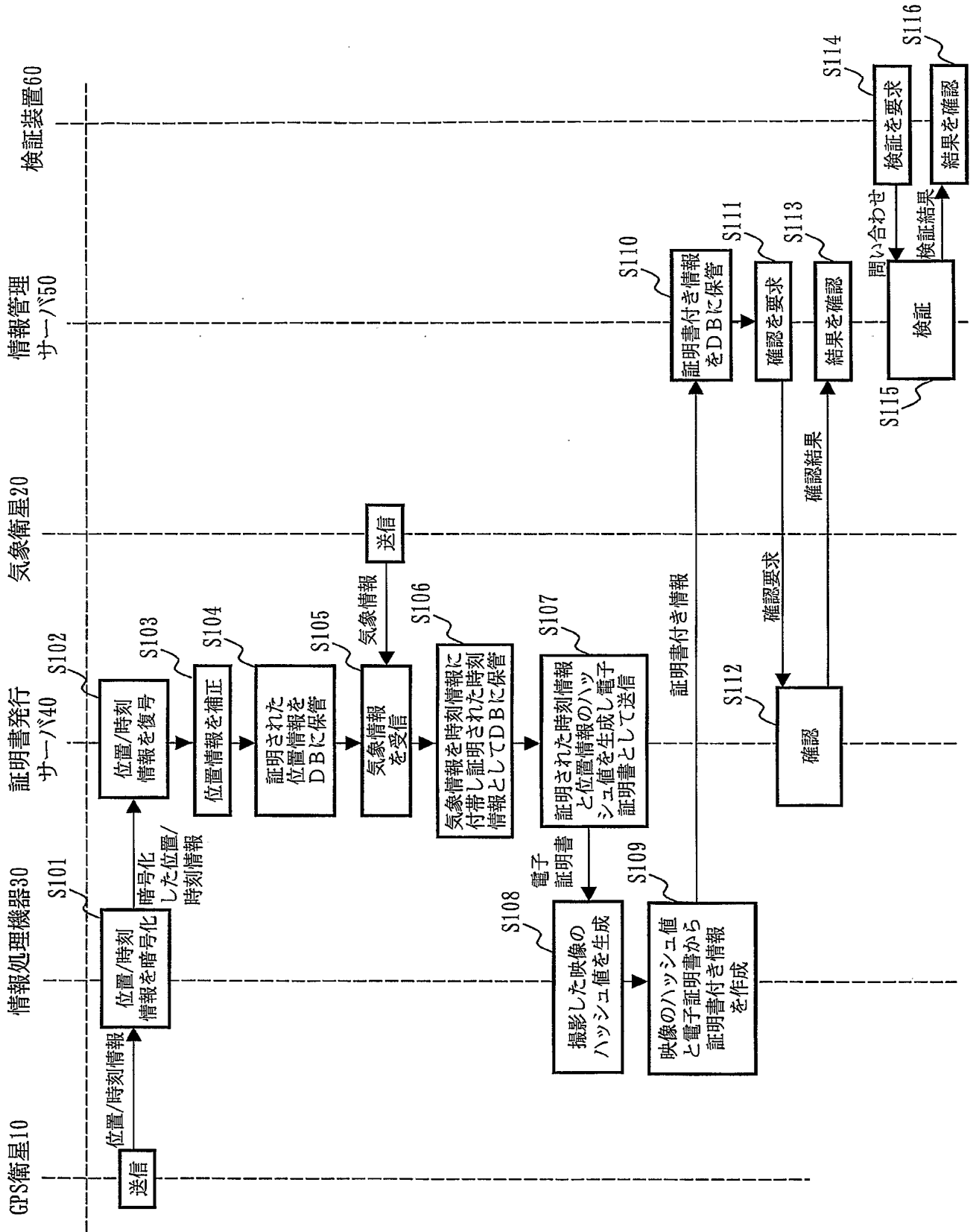
【図 4】



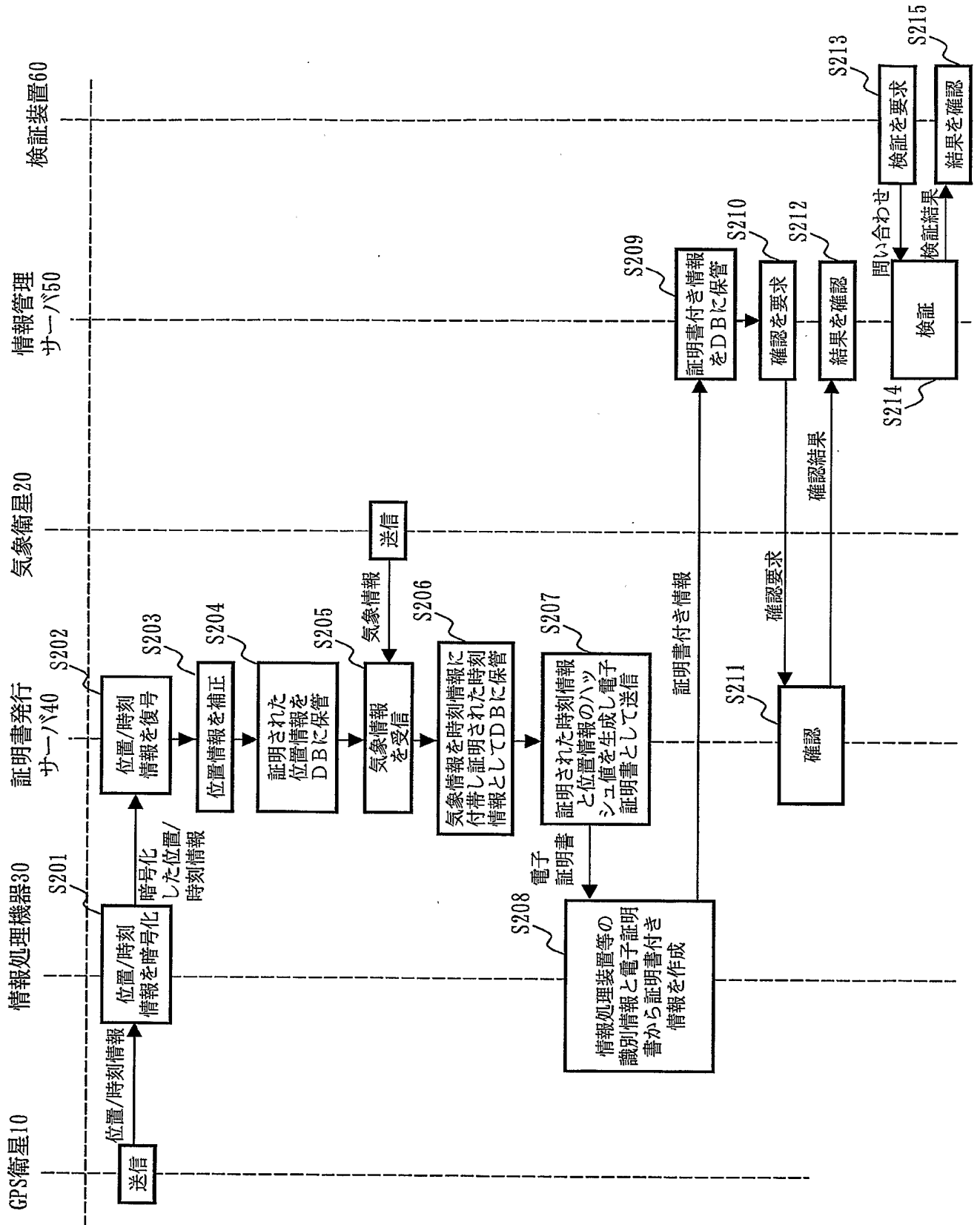
【図 5】



【図 6】



【図 7】



【書類名】 要約書

【要約】

【課題】 例えば、巡回した地点と巡回した時刻を証明する巡回警備の証明システムを提供することを目的とする。また、例えば、証明された地点と時刻の情報を撮影した映像に付加することにより、映像が撮影された地点と時刻を証明することができるようにすることを目的とする。

【解決手段】 地球上の位置情報を提供する G P S 衛星 1 0 と、地球上の気象情報を提供する気象衛星 2 0 と、巡回警備時に携帯する情報処理機器 3 0 と、時刻情報と位置情報との証明を行う証明書発行サーバ 4 0 と、証明された位置情報と時刻情報とそれらを添付した映像を保管する情報保管サーバ 5 0 と、映像を撮影した地点と時刻を検証する検証装置 6 0 と、情報処理機器 3 0 と証明書発行サーバ 4 0 と情報保管サーバ 5 0 と検証装置 6 0 とを相互に接続するネットワーク 7 0 とが存在する。

【選択図】 図 1

特願 2 0 0 4 - 1 6 6 7 0 6

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 6 0 1 3]

1. 変更年月日	1 9 9 0 年 8 月 2 4 日
[変更理由]	新規登録
住 所	東京都千代田区丸の内 2 丁目 2 番 3 号
氏 名	三菱電機株式会社